抗密钥泄露的在线/离线身份基加密机制 *

张秀洁†
(潍坊学院 计算机工程学院, 山东 潍坊 261061)

摘　要：在线离线身份基加密（IBOOE）方案是一种具有高效的密钥生成和加密算法的密码方案。然而，目前已有的 IBOOE 方案无法抵抗边信道攻击，它将引起密码系统秘密信息泄露问题。新方案通过将随机提取器嵌入在线加密算法来隐藏私钥泄露和密文之间的关系，提出首个有界泄露模型下安全的 IBOOE 方案；新方案基于合数阶双线性群上的三个静态假设，利用双系统加密技术在标准模型下抵抗选择明文攻击达到完全安全性和泄露弹性。此外，与传统的 IBOOE 方案相比较，新方案特别适用于敏感数据存储且资源受限的场景。

关键词：基于身份加密；在线/离线；泄露弹性；双系统加密；可证明安全
中图分类号：TP309.7　　doi: 10.19734/j.issn.1001-3695.2018.11.0892

Identity based online/offline encryption resistant to key leakage

Zhang Xiujie†
(*School of Computer Engineering*, *Weifang University*, *Weifang Shandong* 261061, *China*)

Abstract: Identity based online/offline encryption(IBOOE) system is an cryptography scheme of efficient key generation and encryption algorithm. But the exist IBOOE systems can't resilient to side channel attack, it will lead to secret information leakage problem of cryptosystem. This paper embed random extractor to online encryption procedure to mask the relationship between the leakage of secret key and the ciphertext and firstly put forward a bound leakage IBOOE scheme. The proposed scheme employs dual system encryption to prove fully security and chosen plaintext security against key leakage attack in the standard model from three static assumptions on composite order bilinear groups. In addition, compared with the traditional IBOOE scheme, the proposed scheme is extremely suitable for the scenarios where store sensitive data and resource-constrained.

Key words: identity based encryption; online/offline; leakage resilient; dual system encryption; provable security

0　引言

为了解决传统的基于证书的公钥体制中复杂的证书管理问题，Shamir[1]于 1984 年美密会上首次提出基于身份加密（IBE）。在一个 IBE 系统中，用户公钥是基于用户身份的随机串，例如邮箱地址或电话号码。然而 IBE 方案[2~4]必须执行幂乘或双线性对等复杂运算，不适用于无线传感器网络等计算能力非常有限的环境。2008 年 Guo 等人[5]首次提出在线离线身份基加密（IBOOE）方案，将加密过程分解成离线和在线两个阶段，离线阶段在不知道明文和用户身份的前提下，对复杂计算进行预处理输出离线密文；在线阶段获知消息和身份后，仅需少量简单计算即可生成密文，大大提高了在线加密算法的效率，但是其密文长度非常大，不适用于轻量级设备。2009 年 ACNS 会议上，Liu 等人[6]在随机预言机模型（ROM）下，构造了高效的 IBOOE 方案，特别适合计算能力有限的传感器和智能卡等终端设备。2011 年 ASIACCS 会议上 Chow 等人[7]在 ROM 下构造了首个在线/离线身份基密钥封装机制（IBOOKEM），并基于此给出 IBOOE 方案的通用构造。2014 年王等人[20]采用双系统加密系统构造了完全安全的 IBOOE 方案。2015 年 ACISP 会议上，Lai 等人[8]采用新的方法将基于接收者身份的计算量分成离线和在线两个阶段，由 IBOOKEM 给出 IBOOE 的高效半通用构造。2017 年 Lai 等人[9]在 ROM 下提出一个高效的 IBOOE 方案，与以前的方案相比较，它具有较短的密文。

然而，现有的 IBOOE 方案都没有考虑恶意程序的边信道攻击。作为传统的密码系统，假定用户私钥对于可能的攻击来说是完全保密的，但在实际应用中通过边信道攻击（例如时间攻击、能量消耗、冷启动攻击等）可以从保密的私钥或者加密系统内部获取私钥的部分信息。为了模拟上述密钥泄露攻击，泄露弹性密码体制允许攻击者在获得密码方案的部分敏感信息的前提下实现其可证明安全性。2009 年 Akavia 等人[10]首次设计出公钥密码体制下密钥泄露，在用户私钥部分泄露的情况下，方案仍然能够保证安全性。Naor 等人[11]提出有界泄露模型下的公钥加密方案。2010 年，Chow 等人[12]基于 Lekow-Waters 的双系统加密机制[4]，在三个静态假设下给出高效的抗泄露 IBE 方案。文献[13,14]中提出利用双系统加密技术容忍密钥有界泄露，在双线性对群中构造了泄露弹性加密方案。Hazay 等人[15]提出基于任一标准的公钥加密方案构造泄露弹性公钥加密方案的通用转换，基于单向函数构造了泄露弹性伪随机数生成器和泄露弹性消息认证码。为了模拟实际的泄露，假定存在泄露预言机允许敌手访问，从而获取关于私钥的多项式时间可计算函数的输出。近几年，为了抵抗不同的密钥泄露攻击，文献[16~19]提出各种相关的泄露弹性密码原语。

通过分析，已有的 IBOOE 方案无法抵抗密钥泄露攻击，借鉴 Chow 等人[12]提出有界泄露模型刻画密钥泄露攻击，针

收稿日期：2018-11-26；**修回日期：**2019-02-14　**基金项目：**国家自然科学基金资助项目（61802249）；省部级学科平台开放课题资助项目（szjj2015-054）；山东省高等学校科技发展计划资助项目（J16LN56）；潍坊市科技发展计划资助项目（2017GX002）；潍坊学院 2015 年博士科研基金资助项目（2015BS11）

作者简介：张秀洁（1983-），女，山东青州人，讲师，博士，主要研究方向为网络安全与密码学（2008xiujie@163.com）．

对传统的在线/离线身份基加密方案，本文设计了首个泄露弹性在线/离线加密（lrIBOOE）方案。在该机制中，使用在线和离线加密技术提高了系统的计算效率。离线加密预处理复杂计算过程，并保存计算结果为离线密文；轻量级设备执行在线加密算法，利用离线密文仅需少量简单计算即可生成，这里使用随机提取器来隐藏私钥泄露和密文之间的关系，使得敌手即使得到一定量的私钥量也无法攻破 IBOOE 方案，从而达到密钥泄露弹性。此外，基于 Lekow-Waters[4]的双系统加密机制，通过一系列游戏刻画出详细的敌手模型，并在合数阶双线性群上基于三个静态假设证明了游戏之间的不可区分性，从而在标准模型下证明新方案抵抗选择明文攻击达到完全安全性和泄露弹性。

1　预备知识

1.1　统计距离、熵和提取器

定义 1　两个随机变量 X,Y 的统计距离定义为 $SD(X,Y)=1/2\sum_x|Pr[X=x]-Pr[Y=x]|$，其中 $X\overset{stat}{\approx}Y$ 表示 $SD(X,Y)\le\varepsilon$ 表两个随机变量 X、Y 在统计上是不可区分的。$X\overset{stat}{\approx}Y$ 表示统计距离对于安全参数是可忽略的。后者本文称 X,Y 是统计上不可区分的。

定义 2　随机变量 X 的最小熵定义为 $H_\infty(X)=-\log(\max_x Pr[X=x])$，而 X 在随机变量 Y 下的平均条件最小熵 $H_\infty(X|Y)$=-log($E_{y\leftarrow Y}[\max_x \Pr[X=x|Y=y]]$)，其中 $E_{y\leftarrow Y}$ 表示遍历所有 Y 值的期望值。即对所有函数 f, 满足 $\Pr[f(Y)=X]\le 2^{-\tilde{H}_\infty(X|Y)}$，并且存在某个 f 对等号成立。

直观上，随机变量的最小熵是用来衡量任一敌手描述变量的值的困难程度。最小熵越大，则敌手成功的概率越小，因为最优策略是用最大的概率 $\max\Pr[X=x]$来描述变量的值。平均最小熵则是在已知另外一个随机变量的情况下描述随机变量 X 的困难程度。下面的函数称作提取器，它典型应用于构造泄露弹性系统。

定义 3　提取器。一个多项式时间的函数 $ext:G\times\{0,1\}^u\rightarrow\{0,1\}^m$ 是一个平均的(h,ε)强的提取器，如果对随机变量(X,Y)的所有对，满足 $H_\infty(X|Y)\ge h$, $X,Y\in G$，有 $SD((ext(X,U_\mu),U_\mu,Y),(U_m,U_\mu,Y))\le\varepsilon$，其中 G 是一个非空集合，U_μ、U_m 分别是$\{0,1\}^u$、$\{0,1\}^m$ 上的两个均匀分布的随机变量。

1.2　合数阶双线性群

该群是用一个群生成器 G，输入一个安全参数 k 来定义的，它的输出是双线性群的一个具体的描述。本文输出群系统($N=p_1p_2p_3,G,G_T,e$)。其中 $N=p_1p_2p_3$ 为阶，它是 3 个不同的素数的乘积，群 G 和 G_T 是 N 阶循环群。一个双线性映射 $e:G\times G\rightarrow G_T$ 满足下述性质：

a) 双线性。对于任意的 $g,h\in G$, $a,b\in Z_N$，均有 $e(g^a,h^b)=e(g,h)^{ab}$ 成立。

b)非退化性。存在 $g\in G$ 使得 $e(g,g)$在群 G_T 中的阶为 N。

c)可计算性。对于任意 $g,h\in G$，$e(g,h)$可快速求取。

d)正交性。G_1、G_2 和 G_3 表示群 G 中阶分别为 p_1、p_2 和 p_3 的子群，则当 $h_i\in G_i$，$h_j\in G_j$ 且 $i\neq j$，$e(h_i, h_j)$是 G_T 的单位元。具体来说，假设 $h_1\in G_1$，$h_2\in G_2$ ，g 表示 G 中的一个生成元，则有结论 $g^{p_1p_2}$ 能生成群 G_3、$g^{p_1p_3}$ 能生成群 G_2、$g^{p_2p_3}$ 能生成群 G_1。因此对于某些值 $\alpha_1,\alpha_2,h_1=(g^{p_1p_3})^{\alpha_1}$ 和 $h_2=(g^{p_1p_3})^{\alpha_2}$，应满足 $e(h_1,h_2)=e(g^{p_2p_3\alpha_1},g^{p_1p_3\alpha_2})=$ $e(g^{\alpha_1},g^{p_3\alpha_2})^{p_1p_2p_3}=1$，则本文称群 G_1, G_2 和 G_3 的这一特性为正交性。

1.3　困难性假设

在合数阶群上有下面三个困难问题假设。

假设 1　子群判定假设。挑战者运行 $G(1^n)$，生成 $D^1=(N,G,G_T,e,g_1,g_3)$并将其发送给敌手 A。挑战者随机选择 $v\in\{0,1\}$ 和 $(a,b)\leftarrow Z_{p_1}\times Z_{p_2}$，计算 $T_0^1=g_1^a$ 和 $T_1^1=g_1^ag_2^b$，将 T_v^1 发送给 A。最后，敌手 A 输出一个值 v'，如果 $v'=v$，则敌手 A 成功。

本文定义敌手 A 攻击假设 1 的优势为

$$Adv_{G,A}^1(k)=|\Pr[A(D,T_0^1)=1]-\Pr[A(D,T_1^1)=1]|$$

定义 4　称 G 满足假设 1，如果对任意多项式时间敌手 A，有 $Adv_{G,A}^1(k)$ 是关于安全参数 k 的可忽略函数。

假设 2　挑战者运行 $G(1^n)$，随机选择 $(x_1,x_2,x_3)\leftarrow Z_{p_1}\times Z_{p_2}\times Z_{p_3}$，将 $D^2=(N_1,G,G_T,e,g_1,g_3,g_1^{x_1}g_2,g_2^{x_2}g_3^{x_3})$ 发送给敌手 A。挑战者随机选择一个值 $v\in\{0,1\}$，随机选择 $(a,b,c)\leftarrow Z_{p_1}\times Z_{p_2}\times Z_{p_3}$，计算 $T_0^2=g_1^ag_3^c,T_1^2=g_1^ag_2^bg_3^c$，将 T_v^2 发送给 A。最后，敌手 A 输出一个值 v'，如果 $v'=v$，则敌手 A 成功。

本文定义敌手 A 攻击假设 2 的优势为

$$Adv_{G,A}^2(k)=|\Pr[A(D,T_0^2)=1]-\Pr[A(D,T_1^2)=1]|$$

定义 5　称 G 满足假设 2，如果对任意多项式时间敌手 A，有 $Adv_{G,A}^2(k)$ 是关于安全参数 k 的可忽略函数。

假设 3　挑战者运行 $G(1^n)$ 并随机选择 $(x_1,x_2,\beta,z)\leftarrow Z_{p_2}\times Z_{p_2}\times Z_{p_1}\times Z_{p_1}$。将 $D^3=(N_1,G,G_T,e,g_1,g_3,g_1^\beta g_2,\ g_1^zg_2^{x_2},g_2^{y_2})$ 发送给敌手 A。挑战者随机选择 $v\in\{0,1\}$，随机选择 $\eta\leftarrow Z_N$，计算 $T_0^3=e(g_1,g_1)^{\beta z}$ 和 $T_1^3=e(g_1,g_1)^{\beta\eta}$，将 T_v^3 发送给 A。最后，敌手 A 输出一个值 v'，如果 $v'=v$，则敌手 A 成功。

本文定义敌手 A 攻击假设 3 的优势为

$$Adv_{G,A}^3(k)=|\Pr[A(D,T_0^3)=1]-\Pr[A(D,T_1^3)=1]|$$

定义 6　称 G 满足假设 3，如果对任意多项式时间敌手 A，有 $Adv_{G,A}^3(k)$ 是关于安全参数 k 的可忽略函数。

2　泄露弹性身份基在线/离线加密方案的模型定义

2.1　泄露弹性身份基在线/离线加密方案的形式化定义

泄露弹性身份基在线/离线加密（lrIBOOE）方案包括初始化算法 Setup、密钥提取算法 Ext、离线加密算法 Enc^{off}、在线加密算法 Enc^{on} 和解密算法 Dec 五个算法。

a)Setup(1^k)算法。输入系统安全参数 k，输出系统公开参数 PP 和主密钥 MSK。系统参数包括消息集合 M 和密文集合 C。其中，主密钥 MSK 由密钥生成中心秘密存储。

b)Ext(PP,I,MSK)算法。输入系统公开参数 PP、用户的身份信息 I 和系统主密钥 MSK，生成该用户的私钥 SK_I，并通过安全信道将其发送给该用户。

c)Enc^{off}(PP)算法。输入系统公开参数 PP，返回离线密文 CT^{off}。

d)Enc^{on}(M,I,CT^{off},PP)算法。输入消息 M、用户的身份信息 I、离线密文 CT^{off} 和系统公开参数 PP，输出密文 $CT\in C$。

e)Dec(SK_I,CT,PP)算法。输入用户私钥 SK_I、密文 $CT\in C$ 和公开参数 PP，返回消息 $M\in M$ 或⊥。

上述给出的算法要求满足下面的正确性约束条件：对于给定的身份信息 I 和与之对应的私钥 SK_I，有 $Dec(SK_I,Enc^{on}(M,I,Enc^{off}(PP),PP),PP)=M$。

2.2　安全模型

lrIBOOE 方案抵抗选择明文攻击达到完全安全性和泄露弹性，如果任一概率多项式时间（PPT）算法在下面挑战者 B 与敌手 A 游戏 $Game_{Real}$ 中的优势是可忽略的。对于安全参数 k 和泄露参数 $l=l(k)$，游戏 $Game_{Real}$ 定义如下：

初始化阶段。挑战者 B 输入安全参数 k 运行 **Setup(1^k)** 算法，将系统公开参数 PP 返回给敌手 A，秘密保存主私钥 MSK。此外，B 初始化两个集合 $K=\varnothing$ 和 $L=\varnothing$ 分别用于统计密钥提取询问和密钥泄露询问。两个集合 K 和 L 都是身份 I、用户私钥 SK_I 和计数器 $cntr$ 三个元组的集合。即$(I,SK_I,cntr)\in I\times SK\times N$。

阶段 1　敌手 A 适应性地进行如下询问。

a)Ext(I)询问：挑战者 B 运行 **Ext(*PP,I,MSK*)**算法生成对应 I 的用户私钥 SK_I，并将元组$(I, SK_I, 0)$从集合 L 移到 K。

b)Leak(I,h_i)询问：挑战者 B 首先检查是否满足$(I,SK_I,cntr)\in L$，若不满足，则 B 调用 **Ext(*PP,I,MSK*)**算法生成 SK_I，并将元组$(I,SK_I,0)$添加到集合 L 中，然后 B 再检查是否满足 $cntr+l_i\le l$，若满足则将 $h_i(SK_I)$转发给敌手 A，同时设置 $cntr=cntr+l_i$；否则，返回⊥。

c)Reveal(I)询问：挑战者 B 首先检查是否满足$(I,SK_I,cntr)\in L$，若满足，则将元组$(I,SK_I,cntr)$移到集合 K 中，并将私钥 SK_I 转发给敌手 A。若不在集合 L 而在集合 K 中，则 B 泄露 SK_I；若既不在集合 L 也不在集合 K 中，则 B 调用 **Ext(*PP,I,MSK*)**算法生成 SK_I，将元组$(I,SK_I,0)$添加到集合 K 中，并返回 SK_I。

挑战阶段。敌手 A 输出两个等长消息 $M_1,M_2\in M$ 和挑战身份 I^*。挑战者 B 随机选取 $b\in\{0,1\}$，设置 CT^*=**Enc^{on}(*M$_b$*, *I*,Enc^{off}(*PP*),*PP*)**并将 CT^*发送给敌手 A。

阶段 2　同阶段 1，但是不允许敌手 A 进行 Leak(I,h_i)询问和 Reveal(I)询问，继续 Ext(I)询问（$I\neq I^*$）。

猜测阶段。敌手 A 输出对 b 的猜测 b'。如果 $b=b'$，则 A 获胜。

定义 7　如果任何概率多项式时间敌手 A 赢得游戏 Game$_{real}$ 的概率都可以忽略，则称该 lrIBOOE 方案抵抗选择明文攻击达到完全安全性和泄露弹性（IND-lr-CPA）。

3　本文所提出的 lrIBOOE 方案

本文的 lrIBOOE 方案 Σ 由五个算法组成：初始化算法 Setup、密钥提取算法 Ext、离线加密算法 Enc^{off}、在线加密算法 Enc^{on} 和解密算法 Dec。

a)Setup 算法。输入系统安全参数 k。

(a)选取阶为 $N=p_1p_2p_3$ 的双线性群 G，其中 p_1、p_2 和 p_3 是 3 个不同的素数，令 G_i 表示 G 中阶 p_i 的子群，合数阶群的一个双线性映射 $e:G\times G\to G_T$；

(b) 选取一个具有参数 $(\log|G_1|-l,\varepsilon_{ext})$ 的提取函数 ext，随机选取 $u,g,h\in G_1,\alpha,\beta\in Z_N$，选取群 G_3 的生成元 g_3，输出系统公开参数 $PP=(N,G,G_T,e,g,u,h,e(g,g)^\alpha,e(g,g)^\beta,ext)$ 和主密钥 $MSK=(\alpha,\beta,g_3)$。

b)Ext(*PP,I,MSK*)算法。随机选取 $t,r\in Z_N$ 和 $\rho,\rho'\in Z_N$，设置身份 I 的私钥 $SK_I=(k_1,k_2,k_3)=(t,g^\alpha g^{-\beta t}(u^I h)^r g_3^\rho,g^{-r}g_3^{\rho'})$。

c)Enc^{off}(*PP*)算法：随机选取 $s\leftarrow\{0,1\}^u$ 和 $\theta,w,z\in Z_N$，设置 $c_1=s$，计算计算 $c_2=g^z$，$c_3=(u^\theta h)^z$，$c_4=u^{zw}$，$c_5=e(g,g)^{\beta z}$，$c_6=e(g,g)^{\alpha z}$。输出离线密文 $CT^{off}=(c_1,c_2,c_3,c_4,c_5,c_6,w,\theta)$。

d)Enc^{on}(*M,I*, *CT^{off}*,*PP*)算法。输入消息 M，用户身份 I，离线密文 CT^{off} 和公开参数 PP，计算 $c_0=ext(c_1,c_6)\oplus M$，输出密文 $CT=(c_0,c_1,c_2,c_3,c_4,c_5,w_1)$，其中 $w_1=w^{-1}(I-\theta)\bmod Z_N$。

e)Dec(*SK$_I$*, *CT*,*PP*) 算法。给定密文 $CT=(c_0,c_1,c_2,c_3,c_4,c_5,w_1)$，采用用户私钥 SK_I 解密如下：

$$M=c_0\oplus ext(e(k_2,c_2)e(k_3,c_3c_4^{w_1})c_5^{k_1},c_1)$$

正确性验证：

$$\begin{aligned}&c_0\oplus ext(e(k_2,c_2)e(k_3,c_3c_4^{w_1})c_5^{k_1},c_1)\\&=c_0\oplus ext(e(g^\alpha g^{-\beta t}(u^I h)^r g_3^\rho,g^z)e(k_3,c_3c_4^{w_1})e(g,g)^{\beta zt},c_1)\\&=c_0\oplus ext(e(g^\alpha(u^I h)^r,g^z)e(g^{-r}g_3^{\rho'},(u^\theta h)^z(u^{zw})^{w^{-1}(I-\theta)}),c_1)\\&=c_0\oplus ext(e(g^\alpha(u^I h)^r,g^z)e(g^{-r},(u^I h)^z),c_1)\\&=c_0\oplus ext(e(g^\alpha,g^z),c_1)=c_0\oplus ext(c_6,c_1)=M\end{aligned}$$

3.1　半功能材料

半功能密文：假定标准密文 $CT=(c_0',c_1',c_2',c_3',c_4',\ c_5',w_1')$，设 g_2 是子群 G_2 的生成元，选取随机值 $\delta,z_c\leftarrow Z_N\times Z_N$，设置半功能密文为 $CT=(c_0',c_1',c_2'g_2^\delta,c_3'g_2^{\delta z_c},\ c_4'g_2^\delta,c_5',w_1')$。

半功能密钥：假定标准密钥 $SK_I=(k_1',k_2',k_3')$，设 g_2 是子群 G_2 的生成元，选取随机值 $\gamma,z_k\leftarrow Z_N\times Z_N$，设置半功能密钥为 $SK_I=(k_1',k_2'g_2^\gamma,k_3'g_2^{\gamma z_k})$。

3.2　安全模型

这里给出一系列附加的游戏模型 $Game_{Restricted}$、$Leak_i$、KG_i 和 $Game_{Final}$。此外，前面定义的游戏 $Game_{Real}$ 是一个真实的游戏，在这个游戏过程中生成的密文和密钥都是标准的。下面给出游戏模型的刻画。

a)游戏 $Game_{Restricted}$。这是一个限制性游戏，限制敌手不能对模 p_2 后与挑战身份相等的身份的私钥进行密钥查询，即不能询问 $I=I^*\bmod p_2$ 的身份 I 的私钥。这个限制性条件在后续定义的游戏中都成立。

b)游戏 $Leak_i$。令 L 表示 Leak 询问中互不相同的最大的身份数。对于 $i\in$[L-1]，游戏 $Leak_i$ 与游戏 $Game_{Restricted}$ 类似，除了 $Leak_i$ 中的密文是半功能的，并且前 i 个身份（不包含挑战身份）的泄露私钥是半功能的。这里的 Ext 询问的密钥都是标准的。其中，$Leak_0$ 表示构造的所有密钥都是标准的，所有密文都是半功能的；$Leak_{L-1}$ 表示除了挑战身份的私钥外，所有泄露的私钥都是半功能的。

c)游戏 KG_i。令 K 表示 Ext 询问的最大次数。对于 $i\in$[1,K]，游戏 KG_i 构造的密文都是半功能的，除了挑战身份之外所有泄露的密钥都是半功能的，由 Ext 询问生成的前 i 个私钥都是半功能的，剩余的私钥都是标准的。注意，区别于 L 表示不同身份的最大数目，K 是询问的次数。

d)游戏 $Game_{Final}$。与游戏 KG_K 一样，除了密文是一个“修改的”半功能密文。这里，t^*是挑战身份私钥的标签。

$$\begin{aligned}&\sigma\leftarrow\{0,1\},(z,\eta)\leftarrow Z_N\times Z_N,\\&c_0=ext(c_6,c_1)\oplus M_\sigma,c_1\leftarrow\{0,1\}^u,\\&c_6=e(g,g)^{\alpha z}e(g,g)^{\beta(\eta-z)t^*}\\&c_2=g^z g_2^\delta,c_3=(u^\theta h)^z g_2^{\delta z_c},\\&c_4=u^{z\eta}g_2^\delta,c_5=e(g,g)^{\beta\eta},\end{aligned}$$

3.3　安全性证明

基于三个静态困难问题假设，通过证明上面的一系列游戏模型 $Game_{Real}$、$Game_{Restricted}$、$Leak_i$、KG_i 和 $Game_{Final}$ 之间的不可区分性，推导出敌手在实际游戏 $Game_{Real}$ 中的优势可忽略，则在标准模型下 lrIBOOE 方案 Σ 在选择明文攻击的不可区分性游戏中达到 l-密钥泄露安全

定理 1　如果假设 1~3 成立，上面的 lrIBOOE 方案 Σ 抵抗选择明文攻击达到完全安全性和泄露弹性（IND-lr-CPA）。

证明　证明见下面 6 个引理。

引理 2　如果存在敌手 A 使得 $Adv_{\Sigma,A}^{Game_{Real}}-Adv_{\Sigma,A}^{Game_{Restricted}}=\varepsilon$,则可构建一个 PPT 挑战者 B 至少以 $\varepsilon/4$ 的优势攻破假设 1 或假设 2。

证明　B 收到 $D^2=(N_1,G,G_T,e,g_1,g_3,g_1^{x_1}g_2,g_2^{x_2}g_3^{x_3})$ 和 T。B 随机选择 $(x,y,\alpha,\beta)\leftarrow Z_N^4$，令 $u=g^x,h=g^y$，生成公开参数 PP 和主密钥 $MSK=(\alpha,\beta,g_3)$。B 调用算法 **Ext(*PP,I,MSK*)**响应敌手 A 的私

钥询问。

由 $Adv_{\Sigma,A}^{Game_{Real}} - Adv_{\Sigma,A}^{Game_{Restricted}} = \varepsilon$ 知敌手 A 以 ε 的概率询问 $I=I^*\bmod p_2$，即 p_2 整除 $I-I^*$，则 B 通过计算 $a=gcd(I-I^*,N)$得到 N 的一个非平凡因子。设置 $b=N/a$，则分为下面两种情况：

a）$b=p_1$ 或 $b=p_1p_3$。挑战者 B 通过验证 T_v^b 是否是单位元攻破假设 1。

b）$b=p_3$。挑战者 B 通过验证 $e((g_2^{x_2}g_3^{x_3})^b,T_v)$ 是否是单位元攻破假设 2。

通过上述分析，挑战者 B 可以根据 A 的输出区分两种可能的结果，从而确定处于哪个游戏中。但是，根据假设 1 和假设 2 成立，游戏 $Game_{Real}$ 和 $Game_{Restricted}$ 是不可区分的。

引理 3　如果存在 PPT 敌手 A 使得 $Adv_{\Sigma,A}^{Game_{Restricted}} - Adv_{\Sigma,A}^{Leak_0} = \varepsilon$，则可构建一个挑战者 B 以 $\varepsilon/2$ 的优势攻破假设 1。

证明　B 收到 $D^1=(N,G,G_T,e,\ g_1,g_3)$和 T，其中 $T=g_1^a$ 或 $g_1^ag_2^b$。同引理 2 挑战者 B 选择和设置公开参数 PP 和主密钥 MSK。B 调用算法 **Ext(*PP,I,MSK*)**响应敌手 A 的私钥询问。在挑战阶段，A 发送给挑战者 B 两个等长的消息 M_0、M_1 和挑战身份 I^*。挑战者 B 随机选择 $\sigma\leftarrow\{0,1\}$，利用 T 构造挑战密文如下：

$$\begin{aligned}&c_0^*=ext(c_1^*,c_6^*)\oplus M_\sigma,c_1^*\leftarrow\{0,1\}^u,\sigma\leftarrow\{0,1\},\\&(w,\theta)\leftarrow Z_N\times Z_N,c_2^*=T,c_3^*=T^{x\theta+y},c_4^*=T^{\theta w},\\&c_5^*=e(T,g)^\beta,c_6^*=e(T,g)^\alpha,w_1^*=w^{-1}(I^*-\theta)\bmod N\end{aligned}$$

如果 $T=g_1^a$，A 执行游戏 $Game_{Restricted}$；如果 $T=g_1^ag_2^b$，则挑战密文是一个半功能密文且 $z_c=x\theta+y$，由于 z_c 模 p_2 的值与 $x\bmod p_1$ 和 $y\bmod p_1$ 不相关，所以挑战密文的分布是正确的。敌手 A 以 ε 的优势区分游戏 $Game_{Restricted}$ 和 $Leak_0$，则 B 以同样的优势攻破假设 1。通过上述分析，根据假设 1 成立，游戏 $Game_{Restricted}$ 和 $Leak_0$ 是不可区分的。

引理 4　如果存在 PPT 敌手 A 使得 $Adv_{\Sigma,A}^{Leak_{i-1}} - Adv_{\Sigma,A}^{Leak_i} = \varepsilon$，则可构建一个挑战者 B 以 $\varepsilon/2L$ 的优势攻破假设 2。

证明　在挑战阶段之前，B 不确定哪一个身份是挑战身份 I^*，它随机选取 $i^*\leftarrow\{1,2,\dots,L\}$ 作为对挑战身份的猜测，猜对的概率为 $1/L$。则对于第 i^*次私钥询问，B 总用标准密钥响应。

B 收到 $D^2=(N_1,G,G_T,e,g_1,g_3,g_1^{x_1}g_2,g_2^{x_2}g_3^{x_3})$ 和 T，其中 $T=g_1^ag_3^c$ 或 $g_1^ag_2^bg_3^c$。公开参数 PP 和主密钥 MSK 的构造同引理 2。挑战者 B 和敌手 A 交互如下：

密钥询问：

对于前 i-1 个密钥询问，B 选取 $t,r,\rho,\rho',\rho''\in Z_N$，$I$ 表示敌手 A 询问的身份。B 构造私钥如下：

$k_1=t,k_2=g^\alpha g^{-\beta t}(u^Ih)^r(g_2^{x_2}g_3^{x_3})^\rho,k_3=g^{-r}(g_2^{x_2}g_3^{x_3})^{\rho'}g_3^{\rho''}$　对于第 i 个密钥询问，B 选取 $t,\rho\in Z_N$ 和 $z_k=x\theta+y$，采用挑战项 T 构造私钥如下：

$$k_1=t,k_2=g^\alpha g^{-\beta t}T^{z_k}g_3^\rho,k_3=T$$

其中，$t,\rho\leftarrow Z_N\times Z_N$，$z_k=x\theta+y$。

对于其他的密钥询问，B 总用主私钥构造标准密钥来响应。

挑战阶段：当 B 对挑战身份 I^*的猜测不正确则退出；否则 B 随机选择 $\sigma\leftarrow\{0,1\}$，并给 A 返回如下的挑战密文：

$$\begin{aligned}&c_0^*=ext(c_1^*,c_6^*)\oplus M_\sigma,c_1^*\leftarrow\{0,1\}^u,\\&c_2^*=g_1^{x_1}g_2,c_3^*=(g_1^{x_1}g_2)^{x\theta+y},c_4^*=(g_1^{x_1}g_2)^{\theta w},\\&c_5^*=e(g_1^{x_1}g_2,g)^\beta,c_6^*=e(g_1^{x_1}g_2,g)^\alpha,\\&(w,\theta)\leftarrow Z_N\times Z_N,w_1^*=w^{-1}(I^*-\theta)\bmod N\end{aligned}$$

这是合理分布的半功能密文，其中暗含半功能参数 $z_c=x\theta+y$，即 $c_3^*c_4^{*w_1^*}=(g_1^{x_1}g_2)^{x\theta+y}$。在敌手 A 看来，对所有的 $I\neq I^*\bmod N$，$z_c=x\theta+y$ 和 $z_k=x\theta+y$ 是模 p_2 下的随机分布。

如果 $T=g_1^ag_3^c$，A 执行游戏 $Leak_{i-1}$；如果 $T=g_1^ag_2^bg_3^c$，则 A 执行游戏 $Leak_i$。因此，如果敌手 A 以 ε 的优势区分游戏 $Leak_{i-1}$ 和 $Leak_i$，则 B 以 $\varepsilon/2L$ 的优势攻破假设 2。通过上述分析，根据假设 2 成立，游戏 $Leak_{i-1}$ 和 $Leak_i$ 是不可区分的。

引理 5　如果存在 A 使得 $Adv_{\Sigma,A}^{Leak_{L-1}} - Adv_{\Sigma,A}^{KG_1} = \varepsilon$，那么就能构建一个挑战者 B 以 $\varepsilon/2L$ 的优势攻破假设 2。

引理 6　如果存在 A 使得 $Adv_{\Sigma,A}^{KG_{i-1}} - Adv_{\Sigma,A}^{KG_i} = \varepsilon$，那么就能构建一个挑战者 B 以 $\varepsilon/2L$ 的优势攻破假设 2。

证明　引理 5 和 6 的证明与引理 2 和引理 3 的证明类似。这里省略。挑战者以 1/L 的概率猜测挑战身份，为所有泄露的身份 I($I\neq I^*\bmod N$)创建半功能私钥。然后，对于引理 5 和 6 中分别仿真第一阶段的私钥或者第 i 次密钥询问 Ext(I)，挑战者再利用假设 2 的挑战项来构造。第 i 次密钥询问 Ext(I) 之前返回半功能私钥，之后返回标准私钥。这里，注意计数询问次数，而非身份个数。此外，可能在阶段 2 进行第 i 次密钥询问，区别于与泄露询问只在阶段 1。

引理 7　如果存在 A 使得 $Adv_{\Sigma,A}^{KG_K} - Adv_{\Sigma,A}^{Game_{Final}} = \varepsilon$，那么就能构建一个挑战者 B 以 $\varepsilon/2L$ 的优势攻破假设 3。

证明　B 收到 $D^3=(N_1,G,G_T,e,g_1,g_3,g_1^\beta g_2,g_1^zg_2^{x_2},g_2^{y_2})$ 和 T，其中 $T=e(g_1,g_1)^{\beta z}$ 或 $e(g_1,g_1)^{\beta\eta}$。挑战者 B 随机选取 $(x,y,t^*,\tilde{\alpha})\leftarrow Z_N^4$，隐式地包含 $\alpha=\beta t^*+\tilde{\alpha}$，则设置公开参数 $e(g,g)^\beta=e(g_1^\beta g_2,g_1)^\beta,e(g,g)^\alpha=e(g_1^\beta g_2,g_1)^{t^*},u=g^x$，$h=g^y$，并且发送公开参数 PP 给敌手 A。

B 以 1/L 的概率猜对挑战身份 I^*的位置 i^*。

阶段 1　密钥询问：当 A 对身份 I 进行密钥查询时，B 构造身份 I 私钥如下：

当 $I\neq I^{(i^*)}$ 时，B 随机选择 $\tilde{t},\rho,\rho',\rho'',\rho'''\leftarrow Z_N^5$，构造身份 I 的私钥：

$$(t^*-\tilde{t},(g_1^\beta g_2)^{\tilde{t}}g_1^{\tilde{\alpha}}(u^Ih)^rg_3^\rho(g_2^{y_2})^{\rho'''},g_1^{-r}(g_2^{y_2})^{\rho''}g_3^{\rho'})。$$

当 $I=I^{(i^*)}$ 时，B 均匀地随机选择 $r,\rho,\rho'\leftarrow Z_N^3$，构造身份 I 私钥 $(t^*,g_1^{\tilde{\alpha}}(u^{I^{(i^*)}}h)^rg_3^\rho,g_1^{-r}(g_2^{y_2}g_3^{\rho'}))=(k_1^*,k_2^*,k_3^*)$。

挑战阶段：敌手 A 发送给 B 等长消息 M_0 和 M_1。B 随机选择 $\sigma\leftarrow\{0,1\}$，构造挑战密文为

$$\begin{aligned}&c_0^*=ext(c_1^*,c_6^*)\oplus M_\sigma,c_1^*\leftarrow\{0,1\}^u,\\&c_2^*=(g_1^zg_2^{x_2})^{xw},c_3^*=(g_1^zg_2^{x_2})^{x\theta+y},c_4^*=(g_1^zg_2^{x_2})^{\theta w},\\&c_5^*=T,c_6^*=e(k_2^*,c_2^*)e(k_3^*,c_2^*c_4^{*w_1^*})c_4^{*k_1^*},\\&(w,\theta)\leftarrow Z_N\times Z_N,w_1^*=w^{-1}(I^*-\theta)\bmod N\end{aligned}$$

其中: (k_1^*,k_2^*,k_3^*) 是在阶段 1 中为挑战身份 I^*构造的标准私钥。这里设置 $z_c=x\theta+y$，$c_3^*c_4^{*w_1^*}=(g_1^{x_1}g_2)^{x\theta+y}$，因为 x,y 的值只与模 p_1 有关系，z_c 的值只与模 p_2 相关，对于敌手 A 而言，它们看起来是随机的。

如果 $T=e(g_1,g_1)^{\beta z}$，则 A 执行游戏 KG_K;

如果 $T=e(g_1,g_1)^{\beta\eta}$，B 构造的是无效的半功能密文，因为 $e(k_2^*,c_2^*)e(k_3^*,c_2^*c_4^{*w_1^*})c_4^{*k_1^*}=e(g,g)^{\alpha z}e(g,g)^{\beta(\eta-z)t^*}$，则 A 执行游戏 $Game_{Final}$，则 B 以 $\varepsilon/2L$ 的优势攻破假设 2。但是，根据假设 3 成立，所以游戏 KG_K 和 $Game_{Final}$ 是不可区分。

通过引理 2~ 7 的证明，推导得出游戏 $Game_{Real}$、$Game_{Restricted}$、$Leak_i$、KG_i 和 $Game_{Final}$ 之间具有不可区分性，则敌手无法区分真实游戏 $Game_{Real}$ 和游戏 $Game_{Final}$。因此，敌手 A 攻击 lrIBOOE 方案Σ失败，则 lrIBOOE 方案Σ是 IND-lr-CPA 安全的，即

完成定理 1 的证明。

3.4 性能比较

本小节在计算复杂性和存储代价方面对所提方案的效率进行分析，通过标准模型下传统的 IBOOE 方案[5,8,20]进行比较，具体如表 1 所示。其中，E 表示群 G 或 G_T 中的幂指数运算，ME 表示群 G 或 G_T 中的多点乘运算，m_c 是 Z_p^* 或 Z_N 中的模运算，$|G|$表示群 G 中元素的长度。LR 表示泄露弹性。

表 1　性能比较

Table 1　Performance comparison

方案	离线加密	在线加密	安全性模型
文献[5]	$3E$	$1m_c$	选择安全 CPA
文献[8]	$2E$	$1m_c$	选择安全 CPA
文献[20]	$4E$+$1ME$	$1m_c$	完全安全 CPA
本文方案	$4E$+$2ME$	$1m_c$	完全安全 CPA 和 LR

通过表 1，本文的方案中构造的在线加密算法只需一个异或运算和模运算即可生成密文。由于在 Z 中的模运算比群 G 或 G_T 中的幂乘法运算快很多倍，这非常适用于计算能力受限的轻量级设备。本文的方案与文献[20]都采用了双系统加密系统，本文的方案在离线加密阶段增加了 1 个多点乘运算，但是本方案抵抗选择明文攻击达到完全安全性和泄露弹性。此外，在解密过程中，与传统 IBOOE 相比，没有额外增加运算量。通过对比，本文得出本方案在没有增加计算代价的前提下，达到完全安全性和密钥弹性泄露。因此，本文提出的 lrIBOOE 方案在保证效率的同时提供泄露弹性，特别适合于轻量级设备收集敏感数据。

4　结束语

本文首次构造了一个泄露弹性在线/离线身份基加密方案，采用一系列游戏对敌手模型进行了详细刻画，并且采用双系统加密机制，基于合数阶双线性群上的静态假设，在标准模型下对其在密钥泄露环境下的选择明文安全性进行了严格的证明。与现有的 IBOOE 方案相比较，本文方案是高效的和安全的。但是新方案没有考虑适应性选择密文安全性。因此如何基于双系统加密机制，构造抵抗密文攻击的、高效的抗主密钥泄露和用户密钥泄露的 IBOOE 方案是今后研究工作中一个亟待解决的问题。

参考文献：

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-CRYPTO. Berlin: Springer-Verlag, 1984: 47–53.

[2] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles [C]// Advances in Cryptology-EUROCRYPT.Berlin: Springer-Verlag, 2004: 223–238.

[3] Waters B. Efficient identity-based encryption without random oracles [C]// Advances in Cryptology-EUROCRYPT.Berlin: Springer-Verlag, 2005: 114–127.

[4] Lewko A B, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts [C]//Proc of the 7th Theory of Cryptography Conference.Berlin: Springer-Verlag, 2010: 455–479.

[5] Guo Fuchun, Mu Yi, Chen Zhide. Identity-based online/offline encryption [C]// Financial Cryptography and Data Security.Berlin: Springer-Verlag, 2008: 247–261.

[6] Liu J K, Zhou Jianying. An efficient identity-based online//offline encryption scheme [C]// Applied Cryptography and Network Security.Berlin: Springer-Verlag, 2009: 156–167.

[7] CHOW S S, LIU J K, Zhou Jianying. Identity-based online//offline key encapsulation and encryption [C]// Proc of the 6th ACM Symposium on Information, Computer and Communications Security, New York: ACM Press, 2011: 52–60.

[8] Lai Jianchang, Mu Yi, Guo Fuchun, *et al.* Improved identity-based online//offline encryption [C]//Proc of the 20th Australasian Conference Information Security and Privacy: Berlin: Springer-Verlag, 2015: 160–173.

[9] Lai Jianchang, Mu Yi, Guo Fuchun. Efficient identity-based online/offline encryption and signcryption with short ciphertext [J]. International Journal of Information Security, 2017, 16(3): 299–311.

[10] Akavia A, Goldwaser S, Vaikuntanathan V. Simultaneous hardcore bits and cryptography against memory attacks [C]// Proc of the 6th IACR Theory of Cryptography Conference.Berlin: Springer-Verlag, 2009: 474-495.

[11] Naor M, Segev G. Public-key cryptosystems resilient to key leakage [J]. SIAM Journal on Computing, 2012, 41(4): 772–814.

[12] Chow S S M, Dodis Y, Rouselakis Y, *et al.* Practical leakage-resilient identity-based encryption from simple assumptions [C]// Proc of the 17th ACM Conference on Computer and Communications Security.New York: ACM Press, 2010: 152–161

[13] Lewko A B, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption [C]// Proc of the 8th IACR Theory of Cryptography Conference.Berlin: Springer-Verlag, 2011: 70-88

[14] Zhang Mingwu, Yang Bo, Takagi T. Bounded leakage-resilient functional encryption with hidden vector predicate [J]. The Computer Journal, 2013, 56(4): 464-477.

[15] Hazay C, Wee H, Wichs D. Leakage-resilient cryptography from minimal assumptions [J]. Journal of Cryptology, 2016, 29(3): 514-551.

[16] Zhou Yanwei, Yang Bo. Continuous Leakage-resilient public-key encryption scheme with CCA security [J]. Computer Journal, 2017:60 (8) .

[17] Yu Zuoxia, AU MH, Xu Qiuliang, *et al.* Towards leakage-resilient fine-grained access control in fog computing [J]. Future Generation Computer Systems, 2018(78): 763-777.

[18] Li Sujuan, Mu Yi, Zhang Mingwu, *et al.* Continuous leakage resilient lossy trapdoor functions [J]. Information, 2017, 8(2): 38.

[19] Zhang Mingwu, Leng Wentao, Ding Yong, *et al.* Tolerating sensitive-leakage with larger plaintext-space and higher leakage-rate in privacy-aware Internet-of-things [J]. IEEE Access, 2018(99): 1-1.

[20] 王占君，李杰，马海英，等．完全安全的身份基在线/离线加密 [J]. 计算机应用，2014，34(12)：3458-3461. (Wang Zhanjun, Li Jie, Ma Haiying, *et al.* Fully secure identity-based online/offline encryption [J]. Journal of Computer Applications, 2014, 34(12): 3458-3461.)